Amendments to the Claims

1. (CURRENTLY AMENDED) A method of performing an inversion operation in a cryptographic calculation with at least two auxiliary variables, the method comprising shifting ~~(S2)~~ a variable, then effecting a reduction ~~(S3)~~ by subtracting that variable from a larger variable.

2. (ORIGINAL) A method according to Claim 1 wherein the variables are of the same degree.

3. (CURRENTLY AMENDED) A method according to ~~Claim 1 or 2~~ Claim 1 comprising updating a plurality of additional variables such that the invariances remain valid.

4. (CURRENTLY AMENDED) A method according to ~~any preceding claim~~claim 1 comprising four auxiliary variables being U, V, Rand S, having the invariances:

ISV-R.UI = N

SoY = U mQd i\!

R.Y = V mod N.

5. (ORIGINAL) A method according to Claim 4 comprising decreasing U and V in size, step by step until U = 1.

6. (ORIGINAL) A method according to Claim 5 comprising effecting the operation R.Y = 1 mod N or R = y-1 mod N, as appropriate.

7. (CURRENTLY AMENDED) A method according to ~~any preceding claim~~Claim 1 comprising operating with the Most Significant Words of the variables.

8. (CURRENTLY AMENDED) A method according to ~~any preceding claim~~Claim 1 comprising providing inversion ~~(S1-S4)~~ over GF(p).

9. (CURRENTLY AMENDED) A method according to ~~any preceding claim~~Claim 1 comprising providing inversion ~~(S10-S12)~~ over GF(2^n).

10. (CURRENTLY AMENDED) A method according to ~~any preceding claim~~Claim 1 comprising providing a method for long-integer division operations.

11. (CURRENTLY AMENDED) A computer program product directly loadable into the internal memory of a digital computer, comprising software code portions for performing the method of ~~anyone or more of Claims 1 to 10~~Claim 1 when said product is run on a computer.

12. (CURRENTLY AMENDED) A computer program directly load able into the international memory of a digital computer, comprising software code portions for performing the method of ~~anyone of Claims 1 to 10~~Claim 1 when said program is run on a computer.

13. (ORIGINAL) A carrier, which may comprise electronic signals, for a computer program of Claim 12.

14. (ORIGINAL) Electronic distribution of a computer program product of Claim 11 computer program of Claim 12 or a carrier of Claim 13.

15. (CURRENTLY AMENDED) Apparatus for performing an inversion operation in a cryptographic calculation with at least two auxiliary variables, the apparatus comprising means to shift a variable ~~(V, R)~~ and means ~~(10-17)~~ to effect a reduction by subtraction or addition of that variable from a larger variable.

16. (CURRENTLY AMENDED) Apparatus according to Claim 15 wherein the variables ~~(V, R)~~ are of the same degree without shifting.

17. (CURRENTLY AMENDED) Apparatus according to ~~Claim 15 or 16~~ Claim 15 comprising means to update a plurality of additional variables such that the invariance remains valid.

18. (CURRENTLY AMENDED) Apparatus according to ~~any of Claims 15 to 17~~Claim 15 comprising means ~~(10-13)~~ to operate four auxiliary variables being U, V, Rand S, having the invariances:

ISV-RUI = N

S.Y = U mod N

RY=Vmod N.

19. (CURRENTLY AMENDED) Apparatus according to Claim 18 comprising means ~~(10, 11)~~ to decrease U and V in size, step by step until U = 1.

20. (CURRENTLY AMENDED) Apparatus according to Claim 19 comprising means ~~(10-16)~~ to effect the operation RY = 1 mod Nor R = y-1 mod N, as appropriate.

21. (CURRENTLY AMENDED) Apparatus according to ~~any of Claims 15 to 20~~Claim 15 comprising means to operate with the Most Significant Words of the variables.

22. (ORIGINAL) Apparatus for performing an inversion operation in a cryptographic calculation substantially as hereinbefore described with reference to, and/or as illustrated in, anyone or more of the Figures of the accompanying drawings.

23. (ORIGINAL) A method of performing an inversion operation in a cryptographic calculation substantially as hereinbefore described with reference to, and/or as illustrated in, anyone or more of the Figures of the accompanying drawings.